



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/493,984	01/28/2000	Robert S. Eisenbart	18926-003220US	2907

20350 7590 08/10/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/493,984

Applicant(s)

EISENBART ET AL.

Examiner

Michael J. Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 May 2005.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-19 and 21-23 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1,2,4-19 and 21-23 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____

DETAILED ACTION

1. The response of 5/23/2005 was received and considered.
2. Claims 1-2, 4-19 & 21-23 are pending.

Response to Arguments

3. Applicant's arguments filed 5/23/2005 have been fully considered but they are not persuasive.
4. As a general note, Applicant appears to be relying on a specific definition of "signature" so as to differentiate the signature in the claims from the signature as interpreted in the cited art. If Applicant intends to rely on a specific structure to represent the signature or specific process to create the claimed signature, those limitations must be presented in the claims.
5. Applicant's response (p. 8, ¶3) notes that in Gennaro and that the individual blocks are not signed and that the table of cryptographic hashes is created and signed. Further Applicant argues (p. 8, ¶4) that Gennaro does not sign packets, blocks or anything other than the table of hashes and that the cryptographic hash as described and used in Gennaro cannot reasonably be considered to be a digital signature because it cannot be used to verify the identity of the sender. The Examiner respectfully disagrees. The signed table of hashes is in fact a signature on both the table and the individual hashes. Applicant's specification states "The signature 312 is used to verify that portions of both the authorization message 300 and corresponding software message 400 are authentic." The signed table of Gennaro performs this function. By hashing each block and signing the table, a signature is created over the table and the hashes contained in the table. Therefore, Gennaro does disclose generating a signature/signed table over a first

Art Unit: 2134

information/hash table and second information/blocks and sending the signature over the network separately from at least one of the first information or the second information (§1.2, ¶3).

6. Applicant's response (p. 9, ¶3 – p. 10, ¶2) notes that Wong discloses computing a message digest for a packet, including the resulting digest in a second packet and signing the message digest for the second packet concatenated with the previous packet. Applicant's response argues (p. 10, ¶2) that only a single piece of data is signed and therefore Wong does not anticipate the claims. The Examiner respectfully disagrees. Wong's process of (in the instance of the last two packets of the first method) hashing the concatenation of a first packet with the digest of a second packet and signing the resulting hash is generating a signature over a first information and a second information and sending the signature over the network separately from at least one of the first information or the second information. The resulting signature is a signature over both the first and second information (both blocks) and is sent separately from at least one of the blocks. Wong's process of (in the instance of the second method) hashing a list of hashes and signing it anticipates Applicant's claimed "a signature over a first information and a second information" and the signed block digest is sent separately from, for instance, the first block.

7. Applicant's response (p. 11, ¶4) argues that Wasilewski's encryption of the first key with the multi-session key (MSK) and the encryption of the second key with the user's public key does not affect a signature because only the second key is signed. However, Applicant is directed to (col. 9, lines 31-46 & col. 11, lines 4-48) and the rejection stated in the previous Office Action. Wasilewski discloses generating a signature/hash over first information/MSK and second information/control word (col. 9, lines 31-38) and the signature is appended to the control

Art Unit: 2134.

word (in the form of an ECM) (col. 9, lines 41-46) which is sent separately from the first information/MSK.

8. Applicant's response (p. 12, ¶2 – p. 14, ¶2) argues that the combination of Wasilewski and Banker has no supporting motivation (p. 13, ¶1) and does not teach generating a signature over a first information and a second information as recited in claim 1, authenticating the signature over the first and second information as recited in claim 8, or authorization information, wherein a signature is generated over an information object and an authorization information as recited in claim 14 (p. 13, ¶2). However, Banker provides motivation to using an out-of-band channel by teaching that the unit will receive transmissions regardless of the tuned channel (col. 1, lines 28-44 & col. 2, lines 55-68). Further, Wasilewski discloses the alleged missing limitations of the signature over the first and second information as described previously.

9. Applicant's response (p. 15, ¶3 – p. 16, ¶2) argues that Shear teaches that a module may be signed multiple times, but does not disclose a signature covering more than one module. However, Wasilewski's signature is a signature over multiple objects. Shear is cited for teaching the benefits of using multiple signatures, rather than the single signature creating in Wasilewski (Shear, ABSTRACT & col. 7, lines 9-18). Applicant's response further argues that the Office Action provides no motivation for combining Wasilewski, Banker and Shear. However, as stated in the previous Office Action, Shear teaches that generally including multiple signatures reduces vulnerability from an algorithm compromise (Shear, ABSTRACT & col. 7, lines 9-18).

10. Applicant's response (p. 16, ¶3 – p. 18, ¶1) argues that Wasilewski fails to teach the limitations as argued above. However, as described above, Wasilewski '474 is cited for teaching

Art Unit: 2134

those limitations. Wasilewski '866 is cited for teaching the inclusion of tier information in the authorization information (col. 4, lines 51-59). The motivation for modifying Wasilewski '474, as stated in the previous Office Action, is to gain the benefit of controlling access to different tiers of programs in a television subscription service.

11. Applicant's response (p. 18, ¶2 – p. 19, ¶1) argues that the combination Wasilewski '474 and Shear does not teach or suggest the limitations of claim 18. However, the previous Office Action states the rejections of claim 18 and the motivation to combine Wasilewski and Shear (to gain the benefit of controlling access to different tiers of programs in a television subscription service). Applicant has provided no specific argument as to why the rejection is improper and therefore the rejection is maintained for reasons as described here and previously in the instant Office Action.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claims 1 & 8 are rejected under 35 U.S.C. 102(b) as being anticipated “How to Sign Digital Streams” by Gennaro et al. (**Gennaro**). Gennaro discloses generating a signature over first information/hash table and second information/packets, appending the signature to one of the first information or the second information (appended to the hash table), sending the first information/hash table over a network, sending the second information/packets over the network

separately from the step of sending the first information/hash table and sending the signature over the network separately from at least one of the first information/hash table or the second information/packets (separate from the second information/packets) (§1.2, ¶3).

14. Claims 1 & 8 are rejected under 35 U.S.C. 102(e) as being anticipated by “Digital Signatures for Flows and Multicasts”, by Wong et al. (**Wong**).

Regarding claims 1 & 8, Wong discloses generating a signature/block signature ($sign(D_{1-s})$), over first information/first packet (D_1) and second information/second packet (D_2), appending the signature to one of the first information or the second information (appended to each packet), sending the first information/first packet over a network, sending the second information/second packet over the network separately from the step of sending the first information/first packet and sending the signature/block signature over the network separately from at least one of the first information or the second information (signature is sent with later packets also) (p. 504, §2 (intro) and §A Star Chaining).

Regarding claims 1 & 8, Wong discloses generating a signature/ D_{m-i} over first information/second to last packet and second information/last packet, appending the signature to one of the first information or the second information (appended to second to last packet), sending the first information/second to last packet over a network, sending the second information/last packet over the network separately from the step of sending the first information and sending the signature/ D_{m-i} over the network separately from at least one of the first information or the second information (signature is sent with second to last packet) (p. 503, col. 1, ¶5 – col. 2, ¶2).

15. Claims 1-2, 4-6, 8-9, 11-13 & 21 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 5,870,474 to Wasilewski et al. (**Wasilewski**).

Regarding claims 1, 8 & 11, Wasilewski discloses generating a signature/hash over first information/MSK and second information/clear code word (col. 9, lines 31-46), appending the signature/hash to one of the first information or the second information (appended to second information/clear code word) (col. 9, lines 40-46), sending the first information/MSK over a network (col. 11, lines 4-48), sending the second information/clear code word over the network separately from the step of sending the first information (col. 9, lines 40-46) and sending the signature over the network separately from at least one of the first information or the second information (separate from the first information/MSK) (col. 9, lines 31-46 & col. 11, lines 4-48).

Regarding claims 2 & 9, Wasilewski discloses the first information/MSK comprising an authorization data structure/key (col. 9, lines 47-52) and the second information/clear code word comprising a software object/key (col. 9, lines 30-46).

Regarding claim 4, Wasilewski discloses determining which resources a software object in the second information/clear code word is entitled to interact with (which blocks of packets they can decrypt) (col. 8, lines 48-60).

Regarding claim 5, Wasilewski lacks explicitly waiting a predetermined time period after the step of sending the first information before sending the second information. However, it is inherent that, in a packet-based network, a predetermined time period (transmission rate) is waited between each packet, and hence between each piece of information.

Regarding claim 6, Wasilewski discloses the first information/MSK including authorization information for an associated software object/clear code word (col. 9, lines 30-35).

Regarding claim 12, Wasilewski discloses determining a lifetime for which the second information is usable (col. 8, lines 48-60).

Regarding claim 13, Wasilewski discloses checking the first information/MSK for an authorization corresponding to the second information/clear code word (decrypting) (col. 8, lines 25-28).

Regarding claim 21, Wasilewski discloses determining if access of at least one of the first or second information is authorized (determining if control word is authorized) (col. 9, lines 47-58) and ignoring the second information/control word if not authorized (col. 9, lines 47-58).

16. Claims 7, 10, 14-15 & 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski**, as applied to claims 1 and 8 above, in view of U.S. Patent 5,247,364 to Banker et al. (**Banker**).

Regarding claims 7 & 10, Wasilewski discloses a system, but lacks sending information over different transmission pathways. Banker teaches that unlike in-band transactions, out-of-band subscriber terminals receive data over this channel no matter what the channel the subscriber is tuned to (col. 1, lines 28-44 & col. 2, lines 55-68). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include the first information on a different transmission pathway than the second information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the

benefit of delivery regardless of which channel a subscriber was tuned to, as taught by Banker (col. 1, lines 28-44 & col. 2, lines 55-68).

Regarding claim 14, Wasilewski discloses an information object/MSK, authorization information/clear code word wherein a signature/hash is generated over the information object/MSK and the authorization information/clear code word (col. 9, lines 30-38), wherein the signature/hash is integral to one of the information object or the authorization information (integral with the authorization information/ clear code word) (col. 9, lines 40-46). Wasilewski lacks the information object using a first transmission pathway to a set top box, the authorization information using a second transmission pathway to the set top box that is different from the first transmission pathway and the signature using a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways. However, Banker teaches that unlike in-band transactions, out-of-band subscriber terminals receive data over this channel no matter what the channel the subscriber is tuned to (col. 1, lines 28-44 & col. 2, lines 55-68). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include the first information on a different transmission pathway than the second information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of delivery regardless of which channel a subscriber was tuned to, as taught by Banker (col. 1, lines 28-44 & col. 2, lines 55-68).

Regarding claim 15, Wasilewski discloses an authorization message/ECM, which includes the authorization information/clear code word and the signature (col. 9, lines 40-46).

Regarding claim 19, Wasilewski discloses the information object/MSK sent separately over a network from the authorization information/clear code word (col. 11, lines 10-15).

17. Claims 16 & 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski** in view of **Banker**, as applied to claim 14 above, in further in view of U.S. Patent 6,157,721 to Shear et al. (**Shear**). Wasilewski discloses a system, as modified above, that uses digital signatures for verification, but is silent regarding multiple signatures. Shear teaches that using several dissimilar digital signatures, via different algorithms, can reduce vulnerability from algorithm compromise (ABSTRACT & col. 7, lines 9-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of signatures with different signing algorithms in Banker's data and to use one or more of the signatures to validate the data. One of ordinary skill in the art would have been motivated to perform such a modification to reduce vulnerability from algorithm compromise, as taught by Shear (ABSTRACT & col. 7, lines 9-18).

18. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski** in view of **Banker**, as applied to claim 14 above, in further in view of U.S. Patent 5,420,866 to Wasilewski (**Wasilewski '866**). Wasilewski, as modified above, is silent regarding including tiers in the authorization information. However, Wasilewski '866 teaches that satellite and cable access providers include tier information with authorization information sent to decoders to control access to different tiers of programs (col. 4, lines 51-59). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include tier information in the authorization information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of controlling access to different

Art Unit: 2134

tiers of programs in a television subscription service, as taught by Wasilewski '866 (col. 4, lines 51-59).

19. Claims 22 & 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski**, as applied to claims 1 and 8 above, in view of **Shear**. Wasilewski discloses a system that uses digital signatures for verification, but is silent regarding multiple signatures. Shear teaches that using several dissimilar digital signatures, via different algorithms, can reduce vulnerability from algorithm compromise (ABSTRACT & col. 7, lines 9-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of signatures with different signing algorithms in Banker's data and to use one or more of the signatures to validate the data. One of ordinary skill in the art would have been motivated to perform such a modification to reduce vulnerability from algorithm compromise, as taught by Shear (ABSTRACT & col. 7, lines 9-18).

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

Art Unit: 2134

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:


(571) 273-8300
(for formal communications intended for entry)

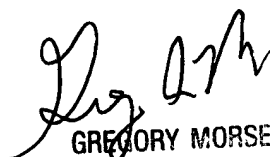
Or:

(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


MJS
July 28, 2005


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER